TRACY L. WILKISON
Acting United States Attorney
CHRISTOPHER D. GRIGG
Assistant United States Attorney
Chief, National Security Division
CAMERON L. SCHROEDER (Cal. Bar No. 255016)
Assistant United States Attorney
Chief, Cyber & Intellectual Property Crimes Section
1500 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-0596
Facsimile: (213) 894-2927
E-mail: cameron.schroeder@usdoj.gov
ADAM ALEXANDER
Assistant United States Attorney
U.S. Attorney's Office for the District of Alaska
222 W. 7th Avenue, Suite 253
Anchorage, AK 99505
Telephone: (907) 271-2309
E-mail: adam.alexander@usdoj.gov

Attorneys for Plaintiff
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

| | |
|---|---|
| UNITED STATES OF AMERICA,<br><br>Plaintiff,<br><br>v.<br><br>MATTHEW GATREL,<br><br>Defendant. | No. CR 19-00036-JAK<br><br>TRIAL MEMORANDUM<br><br>Trial Date: August 26, 2021<br>Trial Time: 8:30 AM<br>Location: Courtroom of the Hon. John A. Kronstadt |

Plaintiff United States of America, by and through its counsel of record, the Acting United States Attorney for the Central District

//

//

Of California and Assistant United States Attorneys Cameron L. Schroeder and Adam Alexander, hereby files its Trial Memorandum.

Dated: August 23, 2021

Respectfully submitted,

TRACY L. WILKISON
Acting United States Attorney

CHRISTOPHER D. GRIGG
Assistant United States Attorney
Chief, National Security Division

/s/
CAMERON L. SCHROEDER
ADAM ALEXANDER
Assistant United States Attorneys

# TABLE OF CONTENTS

DESCRIPTION PAGE

**Contents**

TABLE OF AUTHORITIES.....iii

MEMORANDUM OF POINTS AND AUTHORITIES.....1

I. CASE SCHEDULING MATTERS.....1

II. THE INDICTMENT.....1

III. PRELIMINARY MATTERS.....1

A. Trial Estimate.....1

B. Exhibits; Business and Public Records.....2

C. Co-defendant Juan Martinez.....2

IV. SUMMARY OF THE FACTS.....2

A. Introduction.....2

B. Attack Methodologies.....3

C. AmpNode.....6

D. The FBI Investigation.....8

V. LEGAL AND EVIDENTIARY ISSUES.....10

A. Elements of the Offenses.....10

1. Conspiracy to Cause Damage to Computers.....10

2. Conspiracy to Commit Wire Fraud.....11

3. Unauthorized Impairment of a Protected Computer.....12

B. Defendant's Statements.....13

C. Co-Conspirator Statements.....14

D. Expert Issues.....16

1. Offer of Proof Regarding Expert Witness Testimony...16

a. Prof. Damon McCoy.....16

b. Krassimir Tzvetanov.....17

**TABLE OF CONTENTS (CONTINUED)**


| DESCRIPTION | PAGE |
|---|---|
| 2. Rule 403 and Cumulative Testimony | 19 |
| 3. Rule 703 and Reliance on Inadmissible or Unadmitted Evidence | 21 |
| E. Lay Opinion Testimony | 22 |
| F. Cross-Examination of Defendant | 24 |
| G. Summary Charts | 25 |
| H. Demonstrative Exhibits | 26 |
| I. WHOIS Records | 26 |
| J. Authentication and Identification | 27 |
| VI. FORFEITURE PROCEDURES | 27 |
| A. Overview of Criminal Forfeiture | 27 |
| B. The Property Sought for Forfeiture | 28 |
| C. Relevant Statute Permitting Criminal Forfeiture | 29 |
| 1. Forfeiture Authority Based on Computer Fraud Offenses - 18 U.S.C. § 1030(i)(1) | 29 |
| D. Criminal Forfeiture Procedures | 29 |
| 1. Forfeitability of Property Sought for Forfeiture | 29 |
| 2. Procedural Rules for the Forfeiture Phase and Entry of a Preliminary Order of Forfeiture | 31 |
| VII. CONCLUSION | 34 |

# TABLE OF AUTHORITIES


| DESCRIPTION | PAGE |
|---|---|
| **Federal Cases** | **Page(s)** |
| Am. Online, Inc. v. AOL.org, 259 F. Supp. 2d 449 (E.D. Va. 2003) | 26 |
| Barsky v. United States, 339 F.2d 180 (9th Cir. 1964) | 25 |
| Cantu v. United States, CASE NO. CV 14-00219 MMM (JCGx), 2015 WL 12743881 (C.D. Cal. Apr. 6, 2015) | 20 |
| Columbia Ins. Co. v. seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999) | 26 |
| Crampton v. Ohio, 408 U.S. 941 (1972) | 24 |
| Davis v. United States, No. CV 07-00461 ACK-LEK, 2009 WL 10702627 (D. Haw. Apr. 24, 2009) | 20 |
| Diamond Shamrock Corp. v. Lumbermens Mut. Cas. Co., 466 F.2d 722 (7th Cir. 1972) | 25 |
| EarthLink, Inc. v. Ahdoot, 2005 WL 8154298 (N.D. Ga. Feb. 1, 2005) | 26 |
| Friedman v. Medjet Assistance, L.L.C., No. CV 09-07585-MMM(VBKx), 2010 WL 9081271 (C.D. Cal. Nov. 8, 2010) | 19 |
| Johnson v. United States, 780 F.2d 902 (11th Cir. 1986) | 20 |
| Kaley v. United States, 571 U.S. 320 (2014) | 27-28 |
| Libretti v. United States, 516 U.S. 29 (1995) | 27 |
| McGautha v. California, 402 U.S. 183 (1971) | 24 |
| Nationwide Transp. Fin. v. Cass Info. Sys., 523 F.3d 1051 (9th Cir. 2008) | 22 |

**TABLE OF AUTHORITIES (CONTINUED)**


| DESCRIPTION | PAGE |
|---|---|
| Ohler v. United States, 529 U.S. 753 (2000) | 24 |
| United States v. Ali, 619 F.3d 713 (7th Cir. 2010) | 30 |
| United States v. Ammar, 714 F.2d 238 (3d Cir. 1983) | 15 |
| United States v. Black, 767 F.2d 1334 (9th Cir. 1985) | 24-25, 27 |
| United States v. Bowman, 215 F.3d 951 (9th Cir. 2000) | 14 |
| United States v. Capoccia, 503 F.3d 103 (2d Cir. 2007) | 30, 32 |
| United States v. Chu Kong Yin, 935 F.2d 990 (9th Cir. 1991) | 27 |
| United States v. Collicott, 92 F.3d 973 (9th Cir. 1996) | 13-14 |
| United States v. Creighton, 52 F. App'x 31 (9th Cir. 2002) | 30-31 |
| United States v. Cuozzo, 962 F.2d 945 (9th Cir. 1992) | 24 |
| United States v. Desena, 260 F.3d 150 (2d Cir. 2001) | 15 |
| United States v. Feldman, 853 F.2d 648 (9th Cir. 1988) | 27 |
| United States v. Fernandez, 839 F.2d 639 (9th Cir. 1988) | 14 |
| United States v. Freeman, 498 F.3d 893 (9th Cir. 2007) | 23 |
| United States v. Gadson, 763 F.3d 1189 (9th Cir. 2014) | 23 |
| United States v. Garcia-Guizar, 160 F.3d 511 (9th Cir. 1998) | 31 |

**TABLE OF AUTHORITIES (CONTINUED)**


| DESCRIPTION | PAGE |
|---|---|
| United States v. Gomez, 725 F.3d 1121 (9th Cir. 2013) | 22 |
| United States v. Hernandez-Escarsega, 886 F.2d 1560 (9th Cir. 1989) | 31 |
| United States v. Layton, 720 F.2d 548 (9th Cir. 1983) | 15 |
| United States v. Lazarenko, 476 F.3d 642 (9th Cir. 2007) | 28 |
| United States v. Lechuga, 888 F.2d 1472 (5th Cir. 1989) | 15 |
| United States v. Louthian, 756 F.3d 295 (4th Cir. 2014) | 28 |
| United States v. Messino, 382 F.3d 704 (7th Cir. 2004) | 28 |
| United States v. Meyers, 847 F.2d 1408 (9th Cir. 1988) | 25 |
| United States v. Miguel, 87 F. App'x 67 (9th Cir. Jan. 30, 2004) | 19 |
| United States v. Miranda-Uriarte, 649 F.2d 1345 (9th Cir. 1981) | 24 |
| United States v. Monsanto, 491 U.S. 600 (1989) | 32 |
| United States v. Nava, 404 F.3d 1119 (9th Cir. 2005) | 33 |
| United States v. Newman, 659 F.3d 1235 (9th Cir. 2011) | 32-33 |
| United States v. Nicolo, 597 F. Supp. 2d 342 (W.D.N.Y. 2009) | 33-34 |
| United States v. Ortega, 203 F.3d 675 (9th Cir. 2000) | 13, 14 |
| United States v. Radseck, 718 F.2d 233 (7th Cir. 1983) | 25 |

**TABLE OF AUTHORITIES (CONTINUED)**


| DESCRIPTION | PAGE |
|---|---|
| United States v. Schlesinger, 396 F. Supp. 2d 267 (E.D.N.Y. 2005) | 33 |
| United States v. Soulard, 730 F.2d 1292 (9th Cir. 1984) | 25 |
| United States v. Taylor, 127 F.3d 1108, 1997 WL 661153 (9th Cir. Sept. 25, 1997) | 19 |
| United States v. Turner, 528 F.2d 143 (9th Cir. 1975) | 26 |
| United States v. Vampire Nation, 451 F.3d 189 (3d Cir. 2006) | 28 |
| United States v. Vera, 770 F.3d 1232 (9th Cir. 2014) | 21, 22 |
| United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) | 31 |
| United States v. Yazzie, 976 F.2d 1252 (9th Cir. 1992) | 22 |
| Williams v. Illinois, 132 S. Ct. 2221 (2012) | 21 |
| **Federal Statutes** | |
| 18 U.S.C. § 981 | 32 |
| 18 U.S.C. § 1030 (a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I) | 1, 10 |
| 18 U.S.C. § 1343 | 11 |
| 18 U.S.C. § 1349 | 1, 11 |
| 18 U.S.C. § 1956 | 32 |
| 18 U.S.C. § 2314 | 32 |
| 21 U.S.C. § 853 | 31 |
| **Rules** | |
| Fed. R. Crim. P. 32 | 30 |
| Fed. R. Crim. P. 32.2 | 29, 32, 33 |

**TABLE OF AUTHORITIES (CONTINUED)**


| DESCRIPTION | PAGE |
|---|---|
| Fed. R. Evid. 32.2 | 29, 30 |
| Fed. R. Evid. 106 | 14 |
| Fed. R. Evid. 403 | 19 |
| Fed. R. Evid. 701 | 22, 23 |
| Fed. R. Evid. 702 | 23 |
| Fed. R. Evid. 703 | 21, 22 |
| Fed. R. Evid. 801 | 13, 14 |
| Fed. R. Evid. 803 | 26 |
| Fed. R. Evid. 901 | 27 |
| Fed. R. Evid. 1006 | 25 |

**MEMORANDUM OF POINTS AND AUTHORITIES**

## I. CASE SCHEDULING MATTERS

Trial is set for August 26, 2021 at 8:30 a.m. Defendant Matthew Gatrel is not in custody. The estimated time for the government's case-in-chief is three days. Counsel for defendant have agreed to the authenticity of the government's exhibits but the parties have no other stipulations.

Should the defendant be convicted of either Count One or Count Three, the forfeiture phase of this case would commence, regarding the two domain names that have been seized in connection with this case. Counsel for the defendant have indicated that they do not wish the jury to be retained for this purpose. Information regarding the forfeiture proceedings is detailed below in part VI.

## II. THE INDICTMENT

Defendant is charged in a three-count Indictment with Conspiracy to Commit Unauthorized Impairment of a Protected Computer (18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(VI)), Conspiracy to Commit Wire Fraud (18 U.S.C. § 1349), and Unauthorized Impairment of a Protected Computer (18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(VI)).

The elements for these crimes are detailed below in Section V.

## III. PRELIMINARY MATTERS

### A. Trial Estimate

The government estimates that its case-in-chief will last approximately three court days, depending on cross examination. The government anticipates calling approximately five witnesses in its case-in-chief. The government respectfully requests leave to present

a rebuttal case should defendant present a defense and call witnesses.

**B. Exhibits; Business and Public Records**

The government has noticed its intent to introduce records from Google LLC, Comcast, Cloudflare, and the City of St. Charles pursuant to Federal Rules of Evidence ("FRE") 902(4), (11) (13). The defense had indicated that they do not object to the authenticity of the government's exhibits, but have reserved any other objections.

**C. Co-defendant Juan Martinez**

Co-defendant Martinez has signed a plea agreement in this matter, but has not yet entered his change of plea as of the time of filing. The government may call Mr. Martinez as a witness, and requests that the court conduct the change of plea hearing before Mr. Martinez testifies.

## IV. SUMMARY OF THE FACTS

**A. Introduction**

The government intends to prove at trial the following facts, among others:

Defendant owned and operated two online services accessible via the websites downthem.org ("DownThem") and ampnode.com ("AmpNode"). DownThem allowed customers, for a fee, to launch a type of attack known as a "DDoS" attack on computers connected to the internet by fraudulently appropriating internet bandwidth belonging to legitimate internet servers. DDoS stands for "distributed denial of service," and refers to an attack that enlists other computers to send floods of data to the victim computer, or its corresponding Internet access point. When the volume of data constituting the attack becomes too much for the victim computer to process, it either slows the victim's

Internet connection or causes it to lose it altogether, known as "downing," "booting," or "knocking" the victim from the internet.

The Defendant's DownThem customers could select from a variety of different paid "subscription plans." The subscription plans varied in cost and offered escalating attack capability and allowed them to select different attack durations and relative attack power, as well as the abilitiy to launch simultaneous, or "concurrent" attacks. Once subscribed, even a comparatively unsophisticated customer could launch an attack against any Internet-connected device by typing the appropriate Internet Protocol address, or "IP address," into the intuitive user interface offered by defendant's DownThem website. In addition to the victim IP address, the customer would also select the attack type, attack duration, and the applicable Internet port to target for the attack.

Once a customer entered the information necessary to launch an attack on their victim, defendant's system was set up to use one or more of his own dedicated attack servers to unlawfully appropriate the resources of hundreds or thousands of other servers connected to the internet. Generally, the defendant used various techniques, described in greater detail below, to fraudulently appropriate large volumes of internet bandwidth from legitimate servers configured to be responsive to established Internet protocols in order to provide various services that enhance the functionality of the Internet, and redirect that traffic instead to attack victims on behalf of his clientel.

**B. Attack Methodologies**

For example, "NTP" or "Network Time Protocol" is a protocol that enables Internet-connected devices to establish or synchronize their

clocks. However, NTP and other similarly exploited older Internet protocols have two features that make them vulnerable to abuse from "booter" services like Downthem. The first is that they have programmed responses that can be much larger than the initial query. In practice, this means that a malicious actor can send a very small data request to one of these servers, and receive a very large response. For example, in the NTP scenario, rather than sending a small request saying "What time is it?" and getting a small "It's 6:42 UTC" response, a malicious actor might send a small request along the lines of "What are the IP addresses of the last 600 computers to ask you what time it is?" and receive a very large response with all of that information. This discrepancy in size is referred to as an amplification factor.

The second exploitable feature of these protocols is that they were designed to function using UDP, a "connectionless" Internet communication standard. Normally, devices communicating using the more common TCP protocol go through a three-step process often referred to as a "handshake." This process establishes the protocols of a communication link at the start of a communication between two devices, before full communication begins, and it ensures that the two devices can share data. It also ensures that each of the devices is at the IP address it purports to be, as otherwise the handshake will be misdirected and will not complete. With the UDP standard, no such handshake happens – which allows for faster transmission of data, but also creates the potential for abuse.

In particular, with defendant's scripts abusing one of these protocols, a request would be sent from his attack server on behalf of a paying customer (or for his own attacks), and the response,

rather than going back to defendant's server as would be normal in TCP communications, would instead be directed to the victim device. This process is often referred to as "reflection" – as in, the data request is "reflected" off of the vulnerable server and the response goes to the victim rather than the requester. In addition to using the UDP no-handshake standard, this process depends on a method of disguising one's identity on the Internet known as IP header modification, or "spoofing."

Spoofing allows a user to change information, such as their IP address, in their data packet "headers" – something like changing the return address information on an envelope to make it appear that someone else sent a letter. Through this process, defendant would represent that the requests for the large amounts of data were coming from the victim IP addresses rather than his own server; thus, the large amounts of data would be sent to his customer's attack victims rather than his own servers. Defendant's service was configured to exploit hundreds or thousands of these vulnerable servers whenever a customer launched an attack. He maintained lists of computers that could be abused in this way, referred to as "amp lists" – that is, lists of computers that would send amplified responses to small inquiries using a variety of specific protocols.

Throughout this process, defendant paid only for the usage and bandwidth of his own servers, which were sending out comparatively small requests, requiring only minimum amounts of bandwidth. However, the malicious amplification triggered by those small requests, coupled with the "spoofing" misrepresentation that the request was coming from the victim, caused the vulnerable servers to use a comparatively large amount of bandwidth to send the floods of

data to the victim. In so constructing the attacks, defendant did not have to pay for this large amount of bandwidth, the cost of which was borne by the true owners of the vulnerable servers that were appropriated by the defendant, and the Internet service providers ("ISPs") to which they were connected.

Defendant administered the DownThem site beginning at least as early as October 10, 2014, and continued to do so until the FBI conducted a search at his residence in November of 2018. During that period, defendant was the primary administrator of Downthem, and as a result handled the overwhelming majority of customer service inquiries, reflected in thousands of messages with his customers.

As reflected in these communications, defendant occasionally worked with a variety of other persons who helped run the site or handle customer requests over that time period. Beginning in 2018, one of his customers, co-defendant Juan Martinez, started working with defendant on the DownThem website to improve its functionality. Co-defendant Martinez also began responding to customer support requests, and suggested ideas to defendant on how they could improve the service.

**C. AmpNode**

Defendant's other service, AmpNode, offered a related, but differently structured, functionality. Rather than subscribing to be one of many users of his DownThem service, a customer could obtain their own dedicated attack server from which to launch their own attacks using the amplification and spoofing techniques described above, or to perform network scanning to identify open ports or vulnerable servers.

Defendant would obtain and pre-configure the servers with attack scripts and his amp lists, and sometimes with additional user functionality, so that the customer was set up to launch their own amplified and spoofed attacks. Importantly, defendant obtained these servers from hosting companies that allowed IP header modification, which were often outside the United States, as most reputable providers do not allow spoofing. Some customers would use these servers to set up their own DDoS subscription services, with business models similar to DownThem. In particular, one of his customers ran a site called "Quantum Stresser" that functioned essentially the same way as DownThem, using attack servers obtained via defendant's AmpNode service.

Together, DownThem and AmpNode provided services that caused disruption and damage to tens of thousands of victims during the course of they defendant's conspiracy in a variety of ways. Bandwidth on the internet is a commodity. The third-party victim servers that were conscripted to send the floods of data were triggered to perform puprposeless functions, and to send abnormally large packets of data, which then had to be handled (and the cost absorbed) by their Internet service providers. When the packets from those hundreds or thousands of servers converged on their way to the victims, they had to be absorbed by the victim's ISP. Depending on how they were routed, and what kinds of mitigation procedures were in place, they might cause the victim's computer to have its connection degraded such that the user would be unable to maintain any connection to the Internet or Internet-based services, and would be disconnected from any ongoing Internet service or session. Within a

given network, other computers sharing a switch with the victim could suffer similar impairment.

**D. The FBI Investigation**

The FBI began investigating defendant's services in 2016. As part of the investigation, they set up an account with the DownThem service, paid defendant in Bitcoin for one of the low-tier subscriptions, and proceeded to launch attacks on previously selected computers that could safely handle the attack traffic. For many of these "test" attacks, the FBI recorded the incoming data packets, and investigators were able to observe the resulting quantity of data associated with the attacks and the impact on the computers' performance.

Having empirically and contemporaneously verified that the criminal service functioned as advertised, agents then set about identifying the administrator behind DownThem. They first ascertained that the website was using the services of Cloudflare, a DDoS-mitigation and content-distribution company. Ironically, criminal services such as Downthem oftentimes require DDoS mitigation services to protect from attacks from rival administrators or disgruntled victims.

The FBI received records from Cloudflare showing that the DownThem domain was administered by someone using the email fluffyhostingsolutions@gmail.com. Cloudflare records also showed that the same email was used to administer the related criminal service Ampnode.com. Further investigation revealed that the same IP addresses used to access the Cloudflare accounts were used to access additional gmail accounts, including ampnodehosting@gmail.com and

tankshu04@gmail.com, and that these accounts were linked to each other by recovery email and by "cookie."[1]

A search warrant to Google for those accounts revealed further incriminating evidence, as well as identifying information for defendant. The browsing history showed that the user of the accounts was logging in to both Downthem.org and Ampnode.com and performing administrative tasks. And it contained the name "Matthew Gatrel" in various forms, such as a link to a Venmo account in that name. The emails themselves further corroborated the identification of the defendant as the operator of the Ampnode and Downthem services, as they included emails containing, for example, the name Matthew Gatrel in a subject line or introductory paragraph within the body of the email. They also contained geographical information suggesting that the accountholder lived in St. Charles, Illinois.

Based on this information, agents were able to locate Matthew Gatrel in St. Charles, Illinois, and determine where he was living based on IP address and utility information. As it turned out, defendant had been alternating between two residences, and the agents contacted him at one of the two. They conducted a consensual, non-custodial interview where defendant admitted that he was the administrator for both DownThem and AmpNode, and that he used the email accounts described above. Defendant also provided agents with copies of the databases he used to operate both the DownThem and

---

[1] Cookies are small data files used by websites to track user activity. For example, when a user logs into their Google account from a device, they can choose to save their password and login information locally to avoid the need to manually enter that information every time they access the service. Providers such as Google track log access from multiple accounts using the same device, among other types of information that can be used to identify individuals who may believe they are unidentifiable.

AmpNode websites, as well as files for the websites themselves. These items will be introduced at trial.

Based on that interview and information in the DownThem database, agents were able to determine that shortly before the identification of the defendant as the owner and operator of the Downthem and Ampnode criminal services, another person had been helping to administer the DownThem site, identified by the username Severon. Further investigation led them to identify co-defendant Juan Martinez of Pasadena, California, as Severon. Agents conducted a consensual interview with Mr. Martinez, who also gave them a copy of the DownThem database and, later, access to the email account he used to communicate with the defendant, who he knew by an alias. Mr. Martinez is expected to testify at trial about the purpose of the Downthem DDoS platform, his use of it, and his role in administering it for a brief period prior to the defendant's arrest.

## V. LEGAL AND EVIDENTIARY ISSUES

### A. Elements of the Offenses

#### 1. Conspiracy to Cause Damage to Computers

Defendant is charged in Count One with Conspiracy to Commit Intentional Damage to a Protected Computer, in violation of 18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i). To prove that defendant is guilty of this crime, the government must show: 1) beginning on an unknown date prior to October 10, 2014, and ending on or about November 19, 2018, there was an agreement between two or more persons to commit the crime of Intentional Damage to a Protected Computer; 2) the defendant became a member of the conspiracy knowing of its object and intending to help accomplish it; and 3) one of the members of the conspiracy

performed at least one overt act for the purpose of carrying out the conspiracy.

The elements for Intentional Damage to a Protected Computer, in violation of 18 U.S.C. § 1030(a)(5)(A), are set forth below.

2. Conspiracy to Commit Wire Fraud

Defendant is charged in Count Two with Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. § 1349. To prove that defendant is guilty of this crime, the government must show: 1) beginning on an unknown date prior to October 10, 2014, and ending on or about November 19, 2018, there was an agreement between two or more persons to commit the crime of wire fraud, in violation of 18 U.S.C. § 1343; and 2) the defendant became a member of the conspiracy knowing of its object and intending to help accomplish it.

The elements for Wire Fraud are as follows:

First, the defendant knowingly participated in, devised, or intended to devise a scheme or plan to defraud, or a scheme or plan for obtaining money or property by means of false or fraudulent pretenses, representations, or promises;

Second, the statements made as part of the scheme were material; that is, they had a natural tendency to influence, or were capable of influencing, a person to part with money or property;

Third, the defendant acted with the intent to defraud, that is, the intent to deceive and cheat; and

Fourth, the defendant used, or caused to be used, an interstate or foreign wire communication to carry out or attempt to carry out an essential part of the scheme.

3. Unauthorized Impairment of a Protected Computer

Defendant is charged in Count Three with Unauthorized Impairment of a Protected Computer, in violation of 18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(VI). To prove that defendant is guilty of this crime, the government must show: 1) the defendant knowingly caused the transmission of a program, information, a code, or a command; 2) as a result of the transmission, the defendant intentionally caused damage to a computer without authorization, that is, impaired the integrity or availability of data, a program, a system, or information; and 3) the computer was used in or affected interstate or foreign commerce or communication.[2]

To make this crime a felony, the government must prove that the offense caused impairment to ten or more such computers within a one-year period.

Defendant is also charged with attempt for this crime, as well as aiding and abetting it. To prove that the defendant is guilty of attempt, the government must show: 1) the defendant intended to do the following: (a) knowingly cause the transmission of a program, information, a code, or a command; (b) as a result of the transmission, intentionally cause damage to a computer without authorization, that is, impair the integrity or availability of data, a program, a system, or information; (c) to do so to a computer that was used in or affected interstate or foreign commerce or communication; and (d) to do so to ten or more such computers within a one-year period beginning on or about November 20, 2017; and 2) the defendant did something that was a substantial step toward committing

[2] These elements vary slightly from those in the model instruction, but accurately track the statute itself.

the crime and that strongly corroborated the defendant's intent to commit the crime.

To prove that defendant is guilty of aiding and abetting the crime, the government must show: 1) someone else committed the crime of Intentional Damage to a Protected Computer or Attempting to Commit Intentional Damage to a Protected Computer; 2) the defendant aided, counseled, commanded, induced or procured that person with respect to at least one element of that crime; 3) the defendant acted with the intent to facilitate the crime; and 4) the defendant acted before the crime was completed.

Because defendant was engaged in a conspiracy, he also is liable for this offense if another co-conspirator or co-conspirators committed it, the offense fell within the scope of the unlawful agreement, and it could reasonably have been foreseen to be a necessary or natural consequence of the unlawful agreement.

**B. Defendant's Statements**

The government intends to introduce numerous statements of the defendant, including from his emails, customer support tickets from his website, and statements he made during his interview. These statements are admissible against defendant as statements of a party opponent pursuant to FRE 801(d)(2)(A).

The government's introduction of defendant's statements, however, does not allow defendant to offer his own out-of-court statements. When offered by the defendant, such statements are hearsay. See United States v. Ortega, 203 F.3d 675, 682 (9th Cir. 2000) (district court properly granted the government's motion in limine to exclude defendant's post arrest statements through cross examination of Immigration and Naturalization Service agent); United

States v. Collicott, 92 F.3d 973, 983 (9th Cir. 1996) (hearsay not admitted regardless of Rule 106).

Defendant is not precluded from introducing evidence necessary to put on his defense, but he must do so by testifying. Defendant is not permitted to place any of his prior statements before the Court or jury without subjecting himself to cross-examination. See Ortega, 203 F.3d at 682; United States v. Fernandez, 839 F.2d 639, 640 (9th Cir. 1988). Thus, defendant may not introduce his prior statements through defense witnesses (other than defendant himself) or by cross-examining government witnesses with defendant's hearsay statements.

**C. Co-Conspirator Statements**

Pursuant to FRE 801(d)(2)(E), statements of a co-conspirator are admissible against the defendant if the government shows by a preponderance of the evidence that: (1) a conspiracy existed at the time the statement was made; (2) the defendant had knowledge of, and participated in, the conspiracy; and (3) the statement was made in furtherance of the conspiracy. See United States v. Bowman, 215 F.3d 951, 960-61 (9th Cir. 2000).

The district court may admit statements under Rule 801(d)(2)(E) provided that it does not abuse its discretion. See Bowman, 215 F.3d at 960 (citations omitted). The district court may find that statements were made in furtherance of the conspiracy provided that its factual findings are not clearly erroneous. See id.

Here, the government will seek to admit emails and support ticket communications between defendant and his co-conspirators, including both his customers and other persons helping him run the sites. As defendant repeatedly referenced on his DownThem site and in communications, the DownThem service depended on its subscribers

to be successful; the more people signed up, the more server power defendant could purchase and provide. All of the subscribers were thus co-conspirators, using shared resources for the criminal purpose of conducting DDoS attacks. The AmpNode service performed as an adjuct to the DownThem subscription service, as defendant's communications made clear; he often suggested AmpNode customers use his DownThem service for some of their needs, and suggested DownThem customers who wanted more individualized power and capabilities purchase one of his AmpNode setups. Some customers, like "Andy Rak," clearly used both services simultaneously. Therefore, all such statements of defendant's customers made during and in furtherance of their conspiracy are admissible.

Notably, the phrase "in furtherance of the conspiracy," "must not be applied too strictly or the purpose of the exception would be defeated." United States v. Lechuga, 888 F.2d 1472, 1480 (5th Cir. 1989). There are numerous ways that co-conspirator statements can further of a conspiracy, including, for example,"statements made to keep a conspirator abreast of a co-conspirator's activities," United States v. Layton, 720 F.2d 548, 557 (9th Cir. 1983) overruled on other grounds by United States v. W.R. Grace, 526 F.3d 499 (9th Cir. 2008). See also United States v. Desena, 260 F.3d 150, 158 (2d Cir. 2001) (observing that statements are admissible if they inform a conspirator "as to the progress or status of the conspiracy"); United States v. Ammar, 714 F.2d 238, 252 (3d Cir. 1983) ("[s]tatements between conspirators which . . . inform each other of the current status of the conspiracy"). Many of the statements of defendant's fellow co-conspirators will fall into this category – such as reports

of being able to "down" certain servers or that a certain attack method worked better than others.

**D. Expert Issues**

1. Offer of Proof Regarding Expert Witness Testimony

The defense has moved to exclude or restrict the proposed testimony of the two expert witnesses noticed by the government in this matter. In order to facilitate efficient litigation of these objections, the Court has ordered the government to provide an offer of proof regarding the proposed testimony of each expert, highlighting to the extent possible areas of potential overlap between their proposed testimony and areas where each expert witness will provide unique testimony or perspective in the context of anticipated 403 objections by the defense.

*a. Prof. Damon McCoy*

The first noticed expert is Professor Damon McCoy, a member of the computer science faculty at New York University and a nationally renowned expert in the field of DDoS attacks and the criminal services like Downthem that make those attacks accessible at a price to less technically sophisticated customers. Consistent with the expert disclosure to the defense, the government anticipates that Dr. McCoy will testify from a public-sector academic and research-focused perspective regarding both his general knowledge of this field as well as specific opinions regarding the operation of the defendant's Downthem and Ampnode DDoS for hire services.

As detailed in the expert disclosure sent to the defense on April 28, 2021, the government anticipates that Professor McCoy will testify about the different types of DDoS attacks that are conducted generally, and in that context the space occupied by "booter" or

"stresser" services such as those operated by the defendant in this matter – specifically how those paid subscription services operate; the tiered pricing structure depending on the amount of attack power; and the fraudulent use of amplification and spoofing techniques to appropriate the bandwidth and capacity of innocent third-party servers to conduct those attacks.

Professor McCoy will also testify regarding his review of the back-end databases and websites provided to the government by the defendant in this case and used by him to engage in the charged conduct, describing the differences between the "retail" downthem.com service and the "wholesale" ampnode.com service. He will also testify to his review of the interactions between the defendant and his clientel captured in the customer service communications (or "tickets") stored in the services' databases.

Professor McCoy will also testify to his review of the test attacks conducted by the FBI during the course of the investigation, and the data generated in the course of those attacks and captured in the defendant's databases, third party sensors, and the FBI's records.

Ultimately, Prof. McCoy will testify that in his opinion the services operated by the defendant were indeed capable of performing as advertised, and were in fact used by thousands of clients (and co-conspirators) of the defendant to conduct paid attacks on victims by taking advantage of and appropriating the bandwidth belonging to innocent third-party internet server hosts.

*b. Krassimir Tzvetanov*

The second, and more recently disclosed expert is Krassimir Tzvetanov, a private-sector network engineer has been working in this

field for many years, has attended and spoken at numerous conferences, has published in the field, and is currently pursuing a Ph.D. studying cyber forensics.

Tzvetanov's experience and perspective is materially different from and complimentary to that of Professor McCoy's. While they both share impressive academic credentials specific to the field of computer science, Tzvetanov has private sector experience grappling with the practical implications of DDoS attacks as a private-sector security engineer working for some of the largest internet service providers. His relevant experience includes employment with Fastly, A10 networks, Cisco Systems, Yahoo, and Google, where he accrued significant and practical first-hand experience with DDoS attack mitigation from the perspective of a private-sector internet service provider.

In order to opine on the effects of defendant's services, Mr. Tzvetanov will review much of the same material as Prof. McCoy, including the databases, tickets, and testing and sensor data. However, his testimony will concentrate on the effects of such attacks. He will help the jury understand the systems and processes in place to attempt to deal with DDoS traffic like that created by defendant, including the costs and limitations of such systems. In particular, Mr. Tzvetanov will provide an opinion that defendant's claim that his attacks were consistently mitigated and thus caused no impairment is not accurate.

As is clear from their CV's attached to the disclosure and the government's disclosures themselves, Prof. McCoy and Mr. Tzvetanov, while both highly qualified individually, have substantially different perspectives and experience related to the same field

germane to this jury's deliberations in this matter. Prof. McCoy is a computer scientist and academic who has studied booter services in depth. He is not a network security engineer, as Mr. Tzvetanov is. Mr. Tzvetanov has worked professionally in the field of network security and DDoS mitigation, and can speak directly to the impact on networks of services like defendant's, as well as efforts taken to deal with the problems they create.

2. Rule 403 and Cumulative Testimony

As a result of these differing areas of expertise and resulting testimony, defendant's assertions that the testimony may be cumulative is unfounded. There will be no "needless" presentation of cumulative evidence. See Friedman v. Medjet Assistance, LLC, No. CV 09-07585 MMM VBKX, 2010 WL 9081271, at *6 (C.D. Cal. Nov. 8, 2010) ("Rule 403's cumulative evidence provision does not prohibit the introduction of cumulative evidence; rather, it merely permits courts to exclude cumulative evidence when it has little incremental value.") (quoting United States v. Miguel, 87 Fed. Appx. 67, 68 (9th Cir. Jan.30, 2004) (Unpub. Disp.), and citing United States v. Taylor, 127 F.3d 1108, 1997 WL 661153, *2 (9th Cir. Sept.25, 1997) (Unpub. Disp)). What is more, any potential overlap in the testimony of these experts does not substantially outweigh the probative value of the testimony, as Rule 403 requires for exclusion. Fed. R. Evid. 403. See also Friedman, 2010 WL 9081271 at *6 (testimony of two physicians who reached the same conclusion was not cumulative as their "expertise and testimony is sufficiently distinct that it overcomes defendant's Rule 403 challenge"). This is particularly true for this short trial, which relies substantially on assistance from these experts to interpret the data obtained from defendant

himself. Cf. Davis v. United States, No. CV 07-00461 ACK-LEK, 2009 WL 10702627, at *4 (D. Haw. Apr. 24, 2009) (finding that though two doctors were offered to testify on the same topics and that each doctor's testimony would "essentially be duplicative of the others," they each had different practices and experiences; while they reached some of the same conclusions, they brought "different perspectives to the issues of liability and causation" and in any case, to the extent the testimony was duplicative, it would not unduly prolong the trial, which was short) (internal citations omitted); Johnson v. United States, 780 F.2d 902, 906 (11th Cir. 1986) (holding that the district court abused its discretion in excluding an expert's testimony because, in comparison to other experts, the expert's analysis was somewhat different, his testimony as to a particular issue would have been more comprehensive, and he had different, arguably better, qualifications).

To the extent the Court retains any doubts, the appropriate procedure is to defer ruling until the trial unfolds, if the defendant still objects at the time of testimony. See, e.g., Cantu v. United States, No. CV1400219MMMJCGX, 2015 WL 12743881, at *7 (C.D. Cal. Apr. 6, 2015) (despite overlap between two experts' testimony, the court found that, pretrial, it did not appear "that such overlap will confuse the jury, prejudice Defendant, cause undue delay, or result in needless presentation of cumulative evidence;" nonetheless, if at trial it appeared that needlessly cumulative evidence would be elicited, the objection could be renewed at that time). As the government previously noted, it has no desire to prolong this trial with duplicative testimony – but the evidence in this trial is complex, unintuitive, and likely to be completely foreign to the

jury. The testimony of both experts will be helpful to them in their duties.

3. Rule 703 and Reliance on Inadmissible or Unadmitted Evidence

The government's experts in this case may rely on a variety of otherwise inadmissible evidence. Federal Rule of Evidence 703 outlines the scope of permissible expert testimony, and expressly states that information used to form an expert opinion "need not be admissible for the opinion to be admitted." Instead, an expert witness's use of inadmissible hearsay and testimonial statements is indeed proper where similar experts in that particular field "would reasonably rely on those kinds of facts or data in forming an opinion on the subject." Fed. R. Evid. 703. "Moreover, the expert may disclose to the jury the inadmissible evidence relied on in forming his opinion 'if [its] probative value in helping the jury evaluate the opinion substantially outweighs [its] prejudicial effect.'" United States v. Vera, 770 F.3d 1232, 1237 (9th Cir. 2014)(quoting F. R. Evid. 703).

Supreme Court and Ninth Circuit interpretation of FRE 703 make clear that such use does not run afoul of any Confrontation Clause concerns where the inadmissible information is used in conjunction with the expert's separate knowledge and expertise. Williams v. Illinois, 132 S. Ct. 2221, 2228 (2012) (finding the DNA expert's use of otherwise inadmissible hearsay evidence in forming its expert opinion did not violate the Confrontation Clause); United States v. Vera, 770 F.3d 1232, 1237 (2014) (reasoning that under Rule 703, "there is generally no Crawford problem where an expert 'appli[es]

his training and experience to the sources before him and reach[es] an independent judgment'".)

The experts in this case may rely on statements from others in the field, statements by people who engage in this type of criminal activity, data collected by others in the field, and other evidence that is neither admitted nor potentially admissible. As the Ninth Circuit has made clear, this type of testimony is explicity permissible under FRE 703. See Vera, 770 F.3d at 1239 (testimony appropriate where the expert's testimony clearly "distilled and synthesized what he had learned through his experience") So long as the "expert opinion . . . was not merely repackaged testimonial hearsay but was 'an original product' that could have been 'tested through cross-examination'", such testimony is proper under both the Rules of Evidence and Crawford. Id. (quoting United States v. Gomez, 725 F.3d 1121, 1130 (9th Cir. 2013). Further, it may be necessary to disclose some of the basis for the experts' opinions in order to help the jury understand and evaluate the opinions; the government believes any such evidence, which is likely to be computer-generated data, would have very little prejudicial effect, and thus its probative value would substantially outweigh any such effect.

**E. Lay Opinion Testimony**

"The admissibility of lay opinion testimony under Rule 701 is committed to the sound discretion of the trial judge and his decision will be overturned only if it constitutes a clear abuse of discretion." Nationwide Transp. Fin. v. Cass Info. Sys., Inc., 523 F.3d 1051 (9th Cir.2008) (quoting United States v. Yazzie, 976 F.2d 1252, 1255 (9th Cir.1992)).

While the government's experts will review and interpret many of defendant's and his co-conspirators' statements, Special Agent Peterson will also provide assistance to the jury by explaining the content of many of these statements. In so doing, SA Peterson will not be testifying as an expert; rather, he will be providing lay opinion testimony based on, and informed by, his involvement in this investigation. Such testimony, where based on the law enforcement witnesses' personal observations and direct knowledge of the investigation, falls under FRE 701 and does not qualify as expert testimony governed by FRE 702: lay opinion testimony is admissible if it is (1) "rationally based on the perception of the witness," (2) "helpful to a clear understanding of the witness's testimony or the determination of a fact in issue[,]" and (3) "not based on scientific, technical, or other specialized knowledge within the scope of Rule 702." Fed. R. Evid. 701. See also United States v. Freeman, 498 F.3d 893, 904-05 (9th Cir. 2007) (upholding, as proper lay testimony, detective's testimony interpreting ambiguous statements where his "understanding of ambiguous phrases was based on his direct perception of several hours of intercepted conversations. . . and other facts he learned during the investigation" and his testimony "proved helpful to the jury in determining what [defendants] were communicating during the recorded telephone calls"); United States v. Gadson, 763 F.3d 1189, 1207-08 (9th Cir. 2014) (discussing the appropriateness of lay opnion testimony to interpret recorded conversations, particularly where it is helpful to the jury and not just interpreting ordinary English). SA Peterson's knowledge of defendant's services, gained from his extensive investigation and review of defendant's websites,

databases, attack data, customer support tickets, and emails, and interview with defendant himself, will be uniquely helpful to the jury in understanding the otherwise often cryptic and technical language in defendant's and his co-conspirators' communications. While the experts will be able to explain much of the terminology and import of the communications, only SA Peterson has the knowledge, gained through this investigation, to put the communications in context for the jury.

**F. Cross-Examination of Defendant**

A defendant who testifies at trial waives his right against self-incrimination and subjects himself to cross-examination concerning all matters reasonably related to the subject matter of his testimony. See, e.g., Ohler v. United States, 529 U.S. 753, 759 (2000) (citing McGautha v. California, 402 U.S. 183, 215 (1971) reh'g granted, judgment vacated sub nom. Crampton v. Ohio, 408 U.S. 941 (1972), vacated in part on other grounds, 408 U.S. 941 (1972) ("It has long been held that a defendant who takes the stand in his own behalf cannot then claim the privilege against cross-examination on matters reasonably related to the subject matter of his direct examination")). A defendant has no right to avoid cross-examination on matters which call into question his claim of innocence. United States v. Miranda-Uriarte, 649 F.2d 1345, 1353-54 (9th Cir. 1981). The scope of a defendant's waiver is co-extensive with the scope of relevant cross-examination. United States v. Cuozzo, 962 F.2d 945, 948 (9th Cir. 1992); United States v. Black, 767 F.2d 1334, 1341 (9th Cir. 1985) ("What the defendant actually discusses on direct does not determine the extent of permissible cross-examination or his waiver. Rather, the inquiry is whether 'the government's questions are

reasonably related' to the subjects covered by the defendant's testimony.").

**G. Summary Charts**

Charts and summaries of evidence are governed by Federal Rule of Evidence 1006, which permits the introduction of charts, summaries, or calculations of voluminous writings, recordings, or photographs which cannot conveniently be examined in court. See Fed. R. Evid. 1006. While the underlying documents must be "admissible," they need not be "admitted." See United States v. Meyers, 847 F.2d 1408, 1412 (9th Cir. 1988); United States v. Johnson, 594 F.2d 1253, 1257 n.6 (9th Cir. 1979). Summary charts need not contain the defendant's version of the evidence and may be given to the jury while a government witness testifies concerning them. See United States v. Radseck, 718 F.2d 233, 239 (7th Cir. 1983); Barsky v. United States, 339 F.2d 180, 181 (9th Cir. 1964).

A summary witness may rely on the analysis of others where she has sufficient experience to judge another person's work and incorporate as her own the fact of his or her expertise. The use of other persons in the preparation of summary evidence goes to its weight, not its admissibility. United States v. Soulard, 730 F.2d 1292, 1299 (9th Cir. 1984); see Diamond Shamrock Corp. v. Lumbermens Mutual Casualty Co., 466 F.2d 722, 727 (7th Cir. 1972) ("It is not necessary . . . that every person who assisted in the preparation of the original records or the summaries be brought to the witness stand").

The government intends to introduce summaries/charts of the following records into evidence, each of which is admissible: 1) attack data from the DownThem database; 2) PCAP, or Packet

Capture, data from the FBI's testing of the DownThem service; 3) attack data from the similar database for Quantum Stresser.

**H. Demonstrative Exhibits**

The government may also offer demonstratives that might facilitate the presentation of its evidence, including depictions of the reflection and amplification process, network communications flows, and other jury aids that may make the technological concepts more clear. The admission of demonstrative evidence that assists the understanding of the trier of fact is a matter committed to the sound discretion of the trial court. United States v. Turner, 528 F.2d 143, 167-68 (9th Cir. 1975).

**I. WHOIS Records**

Throughout the course of this trial, witnesses may make reference to WHOIS records. "WHOIS is a public database that courts have relied upon in order to ascertain the party who has registered a domain name." EarthLink, Inc. v. Ahdoot, 2005 WL 8154298, at *8 (N.D. Ga. Feb. 1, 2005). Testimony regarding WHOIS information is admissible under FRE 803(17), which provides an exception to the rule against hearsay for market quotations, lists, directories, or other compilations that are generally relied upon by the public or people in particular occupations. Id. ("WHOIS search results come within the hearsay exception noted in Federal Rule of Evidence 803(17) for directories and other published compilations relied upon by the public."); see also America Online, Inc. v. AOL.org, 259 F. Supp. 2d 449, 452 n.3 (E.D. Va. 2003) (relying on WHOIS records); Columbia Insurance Co. v. SeesCandy.com, 185 F.R.D. 573, 576 (N.D. Cal. 1999) (describing WHOIS as "public database").

**J. Authentication and Identification**

Federal Rule of Evidence 901(a) provides that "the requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Rule 901(a) only requires the government to make a prima facie showing of authenticity or identification "so that a reasonable juror could find in favor of authenticity or identification." United States v. Chu Kong Yin, 935 F.2d 990, 996 (9th Cir. 1991); United States v. Black, 767 F.2d 1334, 1342 (9th Cir. 1985). Once the government meets this burden, "the credibility or probative force of the evidence offered is, ultimately, an issue for the jury." Black, 767 F.2d at 1342.

**VI. FORFEITURE PROCEDURES**

**A. Overview of Criminal Forfeiture**

Criminal forfeiture is imposed on a convicted defendant as part of sentencing. It is not an element of the underlying substantive offense. See Libretti v. United States, 516 U.S. 29, 39 (1995) ("Our precedents have likewise characterized criminal forfeiture as an aspect of punishment imposed following conviction of a substantive criminal offense."); United States v. Feldman, 853 F.2d 648, 662 (9th Cir. 1988) (holding that "trial courts should bifurcate forfeiture proceedings from ascertainment of guilt, requiring separate jury deliberations").

Criminal forfeiture is an important sentencing tool, carrying into effect Congressional intent to deprive criminals and criminal organizations of the instrumentalities and profits of their illegal conduct. See Kaley v. United States, 571 U.S. 320, 323 (2014)

(forfeiture serves to punish the wrong-doer, deter future illegality, lessen the economic power of criminal enterprises, compensate victims, improve conditions in crime-damaged communities, and support law enforcement activities such as police training).

Criminal forfeiture is in personam, in that it may be imposed only after a criminal conviction and applies only to the property of the convicted defendant. See United States v. Lazarenko, 476 F.3d 642, 647 (9th Cir. 2007); United States v. Louthian, 756 F.3d 295, 307 n.12 (4th Cir. 2014) (criminal and civil forfeiture are "distinct law enforcement tools" -- the former is an in personam action that requires a conviction, and the latter is an in rem action against the property itself); and United States v. Vampire Nation, 451 F.3d 189, 202 (3d Cir. 2006) (distinguishing civil and criminal forfeiture).

Finally, the extent of criminal forfeiture is determined by the conviction. The forfeiture must correspond in nature and scope to the underlying criminal conduct for which the defendant was convicted. See United States v. Messino, 382 F.3d 704, 714 (7th Cir. 2004).

**B. The Property Sought for Forfeiture**

The government intends to seek forfeiture of the property set forth in the Indictment, specifically identified as the following Internet domains:

1. downthem.org; and
2. ampnode.com

**C. Relevant Statute Permitting Criminal Forfeiture**

1. Forfeiture Authority Based on Computer Fraud Offenses - 18 U.S.C. § 1030(i)(1)

Section 1030(i) of Title 18 of the United States Code authorizes the criminal forfeiture of personal property that was used or intended to be used to commit or facilitate the commission of a violation or conspiracy to violate Section 1030.

**D. Criminal Forfeiture Procedures**

1. Forfeitability of Property Sought for Forfeiture

The government is required to provide notice of its intent to seek forfeiture in the indictment or information. See Fed. R. Crim. P. 32.2(a) ("A court must not enter a judgment of forfeiture in a criminal proceeding unless the indictment or information contains notice to the defendant that the government will seek forfeiture of property as part of any sentence in accordance with the applicable statute."). The Indictment has provided such notice.

Following conviction, forfeitability of property sought for forfeiture is determined either by the Court or the jury,[3] depending on the election of either party. Rule 32.2(b)(1) provides:

> (A) Forfeiture Determinations. As soon as practical after a verdict or finding of guilty, or after a plea of guilty or nolo contendere is accepted, on any count in an indictment or information regarding which criminal

[3] The right of either party to retain the jury to determine the forfeitability of real or personal property sought for forfeiture is set out at Rule 32.2(b)(5)(A)("In any case tried before a jury, if the indictment or information states that the government is seeking forfeiture, the court must determine before the jury begins deliberating whether either party requests that the jury be retained to determine the forfeitability of specific property if it returns a guilty verdict.").

forfeiture is sought, the court must determine what property is subject to forfeiture under the applicable statute. If the government seeks forfeiture of specific property, the court must determine whether the government has established the requisite nexus between the property and the offense. If the government seeks a personal money judgment, the court must determine the amount of money that the defendant will be ordered to pay.

The forfeiture determination may be based upon evidence already in the record, and on any additional evidence or information submitted by the parties during the forfeiture phase and accepted by the Court as relevant and reliable. See Fed. R. Crim. P. 32(b)(1)(B); United States v. Capoccia, 503 F.3d 103, 109 (2d Cir. 2007) (finder of fact may rely on evidence from the guilt phase; it is not necessary for the government to reintroduce that evidence in the forfeiture phase). To the extent that the government offers new evidence during the forfeiture phase, reliable and relevant hearsay evidence is admissible, as the forfeiture phase of the trial is merely a part of the sentencing process. See United States v. Ali, 619 F.3d 713, 720 (7th Cir. 2010) (because forfeiture is part of sentencing, less stringent evidentiary standards apply in the forfeiture phase of the trial; the evidence need only be "reliable"); Capoccia, 503 F.3d at 109 (Rule 32.2(b)(1) allows the court to consider "evidence or information," making it clear that the court may consider hearsay; this is consistent with forfeiture being part of the sentencing process where hearsay is admissible); United States v. Creighton, 52 Fed. Appx. 31, 35-36 (9th Cir. 2002) (hearsay is

admissible at sentencing and therefore may be considered in the forfeiture phase).

In this case, the parties have agreed not to retain the jury and, instead, have the Court determine forfeiture prior to sentencing.

2. Procedural Rules for the Forfeiture Phase and Entry of a Preliminary Order of Forfeiture

The standard of proof regarding the criminal forfeitability of property is preponderance of the evidence. United States v. Garcia-Guizar, 160 F.3d 511, 518 (9th Cir. 1998) (preponderance standard is constitutional because criminal forfeiture is not a separate offense, but only an additional penalty for an offense that was established beyond a reasonable doubt); United States v. Hernandez-Escarsega, 886 F.2d 1560, 1576-77 (9th Cir. 1989) (interpreting identical language in 21 U.S.C. § 853, the forfeiture statute applicable to most criminal forfeiture proceedings).

At the forfeiture stage, a defendant is not permitted to relitigate the legality of his or her conduct or otherwise attempt to undermine the jury's finding of guilt. United States v. Warshak, 631 F.3d 266, 331 (6th Cir. 2010) (affirming district court's refusal to let defendant introduce evidence tending to show his conduct was not illegal, and holding that in the forfeiture phase the only question is the nexus between the conduct and the offense). The only question to be determined during the forfeiture phase is whether the evidence submitted during the guilt phase, together with any additional evidence received during the forfeiture phase, establishes by a

preponderance of the evidence that there is the requisite nexus[4] between the underlying crime(s) of conviction and the property sought to be forfeited by the government.[5]

If the Court finds that there is such a nexus, it must promptly enter a preliminary order of forfeiture ("POF"). See Fed. R. Crim. P. 32.2(b)(2)(A) ("If the [finder of fact] finds that the property is subject to forfeiture, [the court] must promptly enter a preliminary order of forfeiture ... directing the forfeiture of specific property."); United States v. Monsanto, 491 U.S. 600, 607 (1989) ("Congress could not have chosen stronger words to express its intent that forfeiture be mandatory in cases where the statute applied."); United States v. Newman, 659 F.3d 1235, 1240 (9th Cir. 2011) ("When the Government has met the requirements for criminal forfeiture, the district court must impose criminal forfeiture, subject only to

---

[4] This "nexus" is defined by statute for each offense for which forfeiture is authorized. See e.g., Capoccia, 503 F.3d at 115 ("The 'requisite nexus' for a violation of 18 U.S.C. § 2314 is set forth in 18 U.S.C. § 981(a)(1)(C), which subjects to civil forfeiture '[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to a violation of [various sections of Title 18] or any offense constituting 'specified unlawful activity' (as defined in section 1956(c)(7) of this title), or a conspiracy to commit such offense.'"). Other circuit have defined this nexus as a connection "more than incidental," but "need not be substantial," between the property and the offense. See Seventh Circuit Model Instruction, "Nexus Instruction," available at http://www.ca7.uscourts.gov/pattern-jury-instructions/7th_criminal_jury_instr.pdf, at p. 264

[5] "[F]or example, if the Government is seeking to forfeit the vessel that the defendant used to smuggle drugs, either party may request that the jury be retained to determine whether the Government has established the factual nexus between the vessel and the particular offense on which the defendant was found guilty. In other words, the jury would have to determine whether the vessel was 'used to commit or to facilitate the commission" of the defendant's offense.'" Stefan Cassela, Asset Forfeiture Law in the United States, § 18-4(a).

statutory and constitutional limits"); id. ("[T]he district court has no discretion to reduce or eliminate mandatory criminal forfeiture").

While the POF forfeits the defendant's interest in the property, it does not include a determination of who is the owner of the property subject to forfeiture. That determination is deferred to the ancillary proceedings that follow the entry of the preliminary order, in which any third-party interests in the property are considered and resolved. See Advisory Committee Notes to Federal Rule of Criminal Procedure 32.2 (2000 Adoption) ("Under [the statutory forfeiture scheme first enacted in 1984,] the court orders the forfeiture of the defendant's interest in the property - whatever that interest may be -- in the criminal case. At that point, the court conducts a separate proceeding in which all potential third-party claimants are given an opportunity to challenge the forfeiture by asserting a superior interest in the property. This proceeding does not involve re-litigation of the forfeitability of the property; its only purpose is to determine whether any third party has a legal interest in the forfeited property."); United States v. Nava, 404 F.3d 1119, 1132 (9th Cir. 2005) (district court properly instructed jury that questions of ownership "were not before them").

Because the determination of whether a third party has a legal interest in the forfeited property is made at a separate proceeding, a defendant cannot object to the entry of a POF on the ground that the property at issue does not belong to him. United States v. Schlesinger, 396 F. Supp. 2d 267, 273 (E.D.N.Y. 2005); United States v. Nicolo, 597 F. Supp. 2d 342, 346 (W.D.N.Y. 2009) (in the forfeiture phase of the trial, the court "is not to consider potentially thorny issues concerning third party ownership of

property sought to be forfeited"; if the government establishes the required nexus to the offense, the property must be forfeited).

If the defendant is found guilty of the offenses listed in either Counts One or Three of the Indictment, the government will promptly apply to the Court for entry of a POF forfeiting the defendant's interest in the aforementioned Internet domains, while the defendant reserves the right to oppose the entry of the POF.

**VII. CONCLUSION**

The government respectfully requests leave to file such supplemental memoranda as may become necessary during trial.